

Mirhosseini, M., Magaña-Loaiza, O. S., O'Sullivan, M. N., Rodenburg, B., Malik, M., Lavery, M. P.J., Padgett, M. J., Gauthier, D. J., and Boyd, R. W. (2015) High-dimensional quantum cryptography with twisted light. *New Journal of Physics*, 17(3), 033033.

Copyright © 2015 IOP Publishing Ltd and Deutsche Physikalische Gesellschaft

This work is made available under the Creative Commons Attribution 3.0 License (CC BY 3.0)

Version: Published

<http://eprints.gla.ac.uk/104518/>

Deposited on: 30 March 2015

High-dimensional quantum cryptography with twisted light

This content has been downloaded from IOPscience. Please scroll down to see the full text.

2015 New J. Phys. 17 033033

(<http://iopscience.iop.org/1367-2630/17/3/033033>)

View [the table of contents for this issue](#), or go to the [journal homepage](#) for more

Download details:

IP Address: 130.209.115.82

This content was downloaded on 30/03/2015 at 09:07

Please note that [terms and conditions apply](#).



PAPER

High-dimensional quantum cryptography with twisted light

Mohammad Mirhosseini¹, Omar S Magaña-Loaiza¹, Malcolm N O'Sullivan¹, Brandon Rodenburg¹, Mehul Malik^{1,2}, Martin P J Lavery³, Miles J Padgett³, Daniel J Gauthier⁴ and Robert W Boyd^{1,5}¹ The Institute of Optics, University of Rochester, Rochester, New York 14627, USA² Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Boltzmanngasse 3, A-1090 Vienna, Austria³ School of Physics and Astronomy, University of Glasgow, Glasgow, G12 8QQ, UK⁴ Department of Physics, Duke University, Durham, NC 27708 USA⁵ Department of Physics, University of Ottawa, Ottawa ON K1N 6N5, CanadaE-mail: mirhosse@optics.rochester.edu**Keywords:** quantum key distribution, orbital angular momentum, singular optics

RECEIVED

5 October 2014

REVISED

15 January 2015

ACCEPTED FOR PUBLICATION

16 February 2015

PUBLISHED

20 March 2015

Content from this work
may be used under the
terms of the [Creative
Commons Attribution 3.0
licence](#).

Any further distribution of
this work must maintain
attribution to the
author(s) and the title of
the work, journal citation
and DOI.

**Abstract**

Quantum key distribution (QKD) systems often rely on polarization of light for encoding, thus limiting the amount of information that can be sent per photon and placing tight bounds on the error rates that such a system can tolerate. Here we describe a proof-of-principle experiment that indicates the feasibility of high-dimensional QKD based on the transverse structure of the light field allowing for the transfer of more than 1 bit per photon. Our implementation uses the orbital angular momentum (OAM) of photons and the corresponding mutually unbiased basis of angular position (ANG). Our experiment uses a digital micro-mirror device for the rapid generation of OAM and ANG modes at 4 kHz, and a mode sorter capable of sorting single photons based on their OAM and ANG content with a separation efficiency of 93%. Through the use of a seven-dimensional alphabet encoded in the OAM and ANG bases, we achieve a channel capacity of 2.05 bits per sifted photon. Our experiment demonstrates that, in addition to having an increased information capacity, multilevel QKD systems based on spatial-mode encoding can be more resilient against intercept-resend eavesdropping attacks.

1. Introduction

First introduced in 1984 by Bennett and Brassard, quantum key distribution (QKD) is a method for distributing a secret key between two parties [1, 2]. Due to a fundamental property of quantum physics known as the no-cloning theorem, any attempt made by a third party to eavesdrop inevitably leads to errors that can be detected by the sender and receiver [3, 4]. Modern QKD schemes conventionally use a qubit system for encoding information, such as the polarization of a photon. Such systems are easily implemented because technology for encoding and decoding information in a qubit state-space is readily available today, enabling system clock rates in the GHz regime [5–7]. Recently, the spatial degree of freedom of photons has been identified as an extremely useful resource for transferring information [8, 9]. The information transfer capacity of classical communication links has been increased to more than one terabit per second using spatial-mode multiplexing [10]. In addition, it has been theoretically shown that employing multilevel quantum states (qudits) can increase the robustness of a QKD system against eavesdropping [11–14]. Although the majority of high-dimensional QKD schemes so far have employed time-bin encoding for increasing the alphabet size [15–18], it is expected that spatial-mode encoding can be alternatively used to enhance the performance of a QKD system considering the recent advances in free-space orbital angular momentum (OAM) communication, .

The feasibility of high-dimensional QKD in the spatial domain has been previously demonstrated by encoding information in the transverse linear momentum and position bases [19, 20]. While such encoding schemes provide a simple solution for increasing the information capacity, they are not suitable for long-haul optical links due to the cross-talk caused by diffraction. Diffraction creates a varying transmission loss for

different spatial frequencies that results in mixing of spatial modes [21, 22]. Cross-talk increases the quantum symbol error rate (SER) and fundamentally limits the secure key rate of a QKD system. This adverse effect can be alleviated by employing OAM modes. Due to their rotational symmetry, OAM modes have the desirable property of remaining orthogonal upon propagation in a system with round apertures [23]. In a recent experiment, OAM modes were used for performing classical communication over a 3 km long free-space optical link [24]. In this experiment, the main contribution of turbulence was shown to be a transverse displacement of the OAM modes i.e., a tip-tilt error that can be readily corrected for with present technology. As such, OAM modes are ideal candidates for use in a free-space quantum communication link.

The OAM of photons has enabled many applications in the field of quantum information including studies of quantum entanglement [25–28], photonic superdense coding [29], realization of high-dimensional wavefunctions [30], and quantum cloning [31]. Similarly, a number of studies have investigated the benefits of employing OAM modes in quantum cryptography [32–34]. Recently, rotation-invariant OAM vector modes have been used for performing QKD in a two-dimensional state space [35]. Although this method offers an advantage in terms of optical alignment, it fails to utilize the large information capacity of the OAM basis. The complete realization of a high-dimensional QKD system with OAM has remained impractical up until now mostly due to the difficulty in efficiently sorting single photons in the OAM basis. Additionally, any realistic application requires a fast key-generation rate that cannot be achieved with most of the common methods for generating OAM modes.

2. High-dimensional QKD with OAM

In this paper we describe a proof-of-principle experiment that demonstrates the feasibility of performing high-dimensional quantum cryptography with OAM modes. We encode information in a seven-dimensional set of OAM modes along with modes in the mutually unbiased basis of azimuthal angle (ANG). Our scheme uses a digital micro-mirror device (DMD) for fast generation, and an efficient technique for unambiguous sorting of both OAM and ANG modes. By combining these techniques, we selectively generate the set of 14 spatial modes at a rate of 4 kHz and correspondingly detect them with a separation efficiency of 93 %. We measure a channel capacity of 2.05 bits per sifted photon with an average SER of 10.5 % that is well below the error bounds that are required for security against intercept-resend eavesdropping attacks. Of our SER, 4% is due to detector dark counts and ambient light, and 6.5% is due to errors due to intermodal crosstalk.

In our scheme, Alice randomly chooses her photons from two complementary bases. The primary encoding basis is a set of OAM vortex modes. These modes have a top-hat intensity structure and a helical phase profile characterized by $\Psi_{\text{OAM}}^{\ell} = e^{i\ell\varphi}$, where $\ell \in \{-3; 3\}$ (see figure 1). We construct a mutually unbiased basis set using a linear combination of OAM modes of index $|\ell| \leq 3$ with equal amplitudes

$$\Psi_{\text{ANG}}^n = \frac{1}{\sqrt{d}} \sum_{\ell=-N}^N \Psi_{\text{OAM}}^{\ell} \exp\left(\frac{i2\pi n\ell}{d}\right), \quad (1)$$

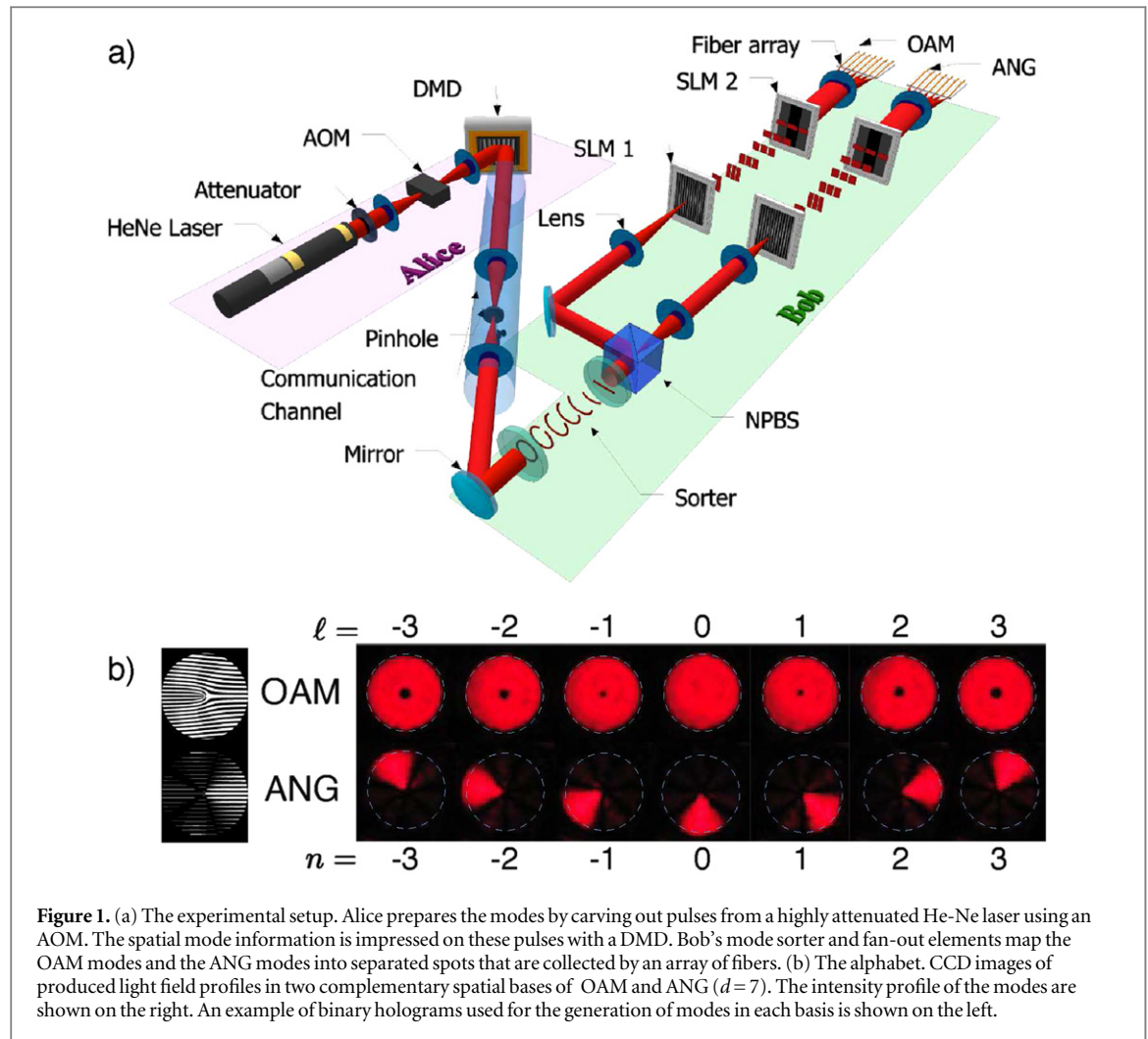
where the dimension $d = 2N + 1 = 7$ in our experiment. We refer to these modes as the angular (ANG) modes due to their localized intensity patterns (see figure 1). The ANG modes form a mutually unbiased basis with respect to the OAM basis [36–38]

$$\left| \left\langle \Psi_{\text{ANG}}^n \middle| \Psi_{\text{OAM}}^{\ell} \right\rangle \right|^2 = 1/d \quad \forall \{n, \ell\}. \quad (2)$$

Consequently, the measurement of a photon in the ANG basis provides no information about its OAM state and vice versa. Additionally, the ANG and the OAM bases remain mutually unbiased upon propagation (See appendix).

Our experimental setup is depicted in figure 1. A collimated beam from a helium–neon laser illuminates a binary hologram realized on a DMD to generate spatial modes [39]. We use a prepare-and-measure scheme similar to the BB84 protocol [1]. Alice initially picks a random sequence of desired OAM and ANG modes and loads the binary holograms for generating each of the modes in the sequence to the DMD’s internal memory. To transmit each symbol, Alice then triggers the DMD and modulates the beam using an acousto-optic modulator to create rectangular pulses of 125 ns width. The beam power is attenuated such that each pulse contains on average $\mu = 0.1$ photons. The prepared states are then imaged to Bob’s receiving aperture via a 4f telescope that forms a lossless 2 m long communication link.

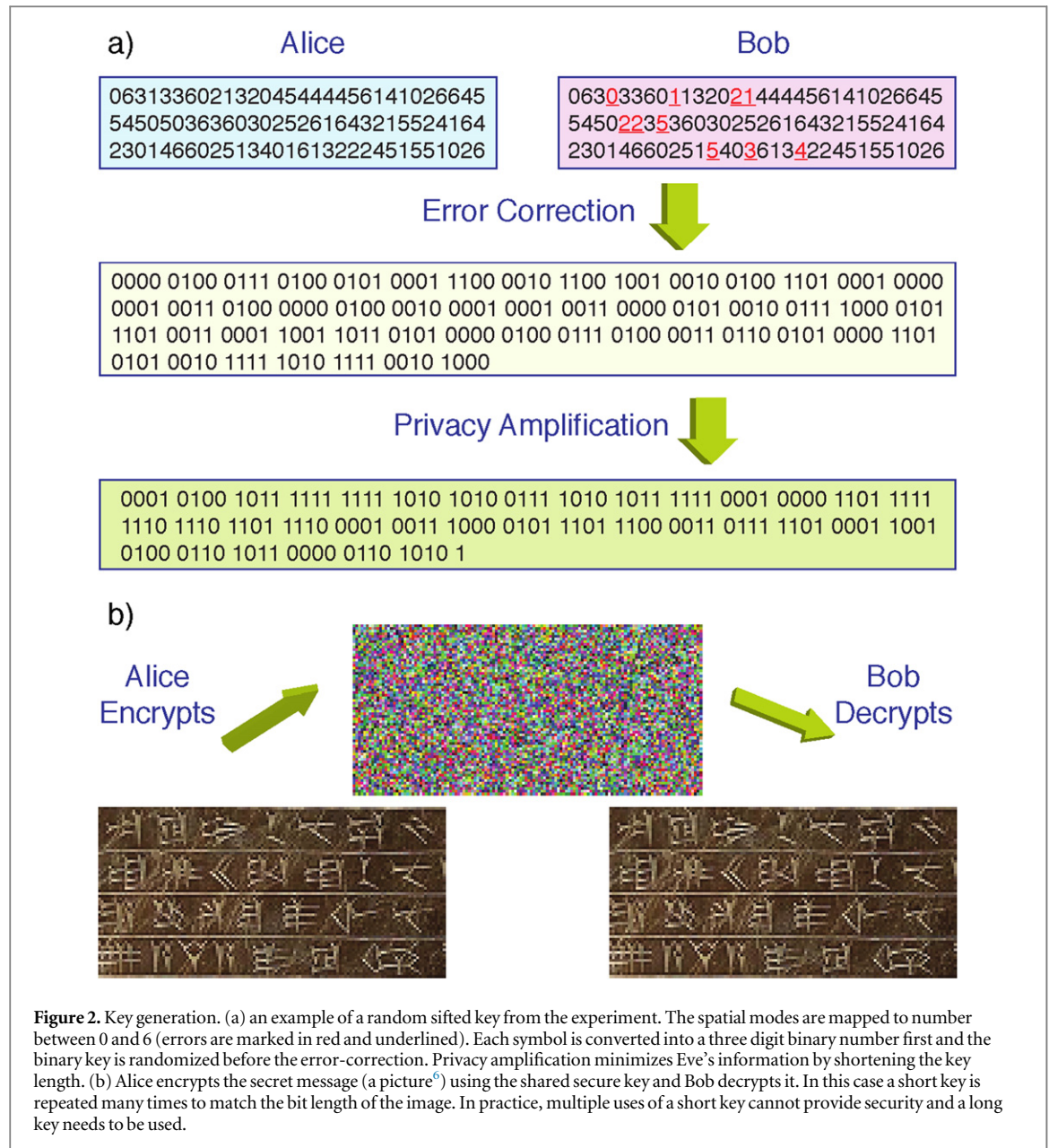
Bob’s mode sorter consists of two refractive elements for performing a log-polar to cartesian transformation [40]. Going through these elements, an OAM mode is converted to a plane wave with a tilt that is proportional to the OAM mode index ℓ . A single lens focuses such a plane wave into a spot that is shifted by an amount proportional to ℓ . Similarly, an ANG mode transforms to a localized spot shifted by an amount proportional to



the angular index n . A beam splitter is used to randomly choose between the OAM and ANG bases. In order to reduce the overlap between the neighboring transformed modes, we use a coherent beam combination technique [41]. A fan-out element is realized on a phase-only spatial light modulator (SLM) to divide the incident light into multiple copies. The copies are phase corrected using a second SLM and are recombined by a lens to a series of much narrower spots with the same initial spacing between them. In addition, two cylindrical lenses are realized on the SLMs to adjust the aspect ratio of the transformed modes.

The sorted modes are coupled to an array of fibers that are connected to avalanche photodiodes (APDs). Due to the limited number of available APDs (four), Bob's data for each group of the symbols is taken separately and is combined later. The signal from the APDs is processed by a field-programmable gate array to produce photon counts using a gating signal shared with Alice. The photon detection events are finally saved in Bob's computer. Alice and Bob are also connected via a classical link realized by an ethernet cable running a TCP/IP protocol. After Alice and Bob collect a sufficiently large number of symbols, they stop the measurement. At this point, they publicly broadcast the bases used for preparation and measurement of each photon via the classical link. Alice and Bob then discard the measurements that were done in different bases. The key generated at this stage is referred to as the sifted key.

Figure 2 shows a portion of the sifted key generated in the experiment. At this stage, the two copies of the key owned by Alice and Bob are almost identical but they contain some discrepancies. The discrepancies are due to the imperfections in our system, namely imperfect mode-sorting, detector dark counts, and ambient light. However, any errors in the key must be attributed to an eavesdropper and corrected for using the procedure of error correction. The keys are transformed to a binary form on a symbol-by-symbol basis and randomized by means of a random-number generator shared by Alice and Bob. The cascade protocol is run by Alice and Bob to fix the discrepancies by comparing the two keys in a block-by-block fashion and performing parity checks [42]. After error-correction, Alice and Bob share two identical copies of the key. However, a portion of the key can still be known to Eve from eavesdropping on the quantum channel or from accessing the publicly available information transmitted in the classical channel during the error correction. Alice and Bob perform privacy



amplification to minimize Eve's information. This is done by using a universal hash function for mapping the error-corrected key to a shorter random key of desired length [43]. The amount by which the key is shortened at this stage is chosen by estimating the amount of information owned by Eve. Finally, the secure key is used to securely transmit information (a picture in this case) over the classical channel (see figure 2).

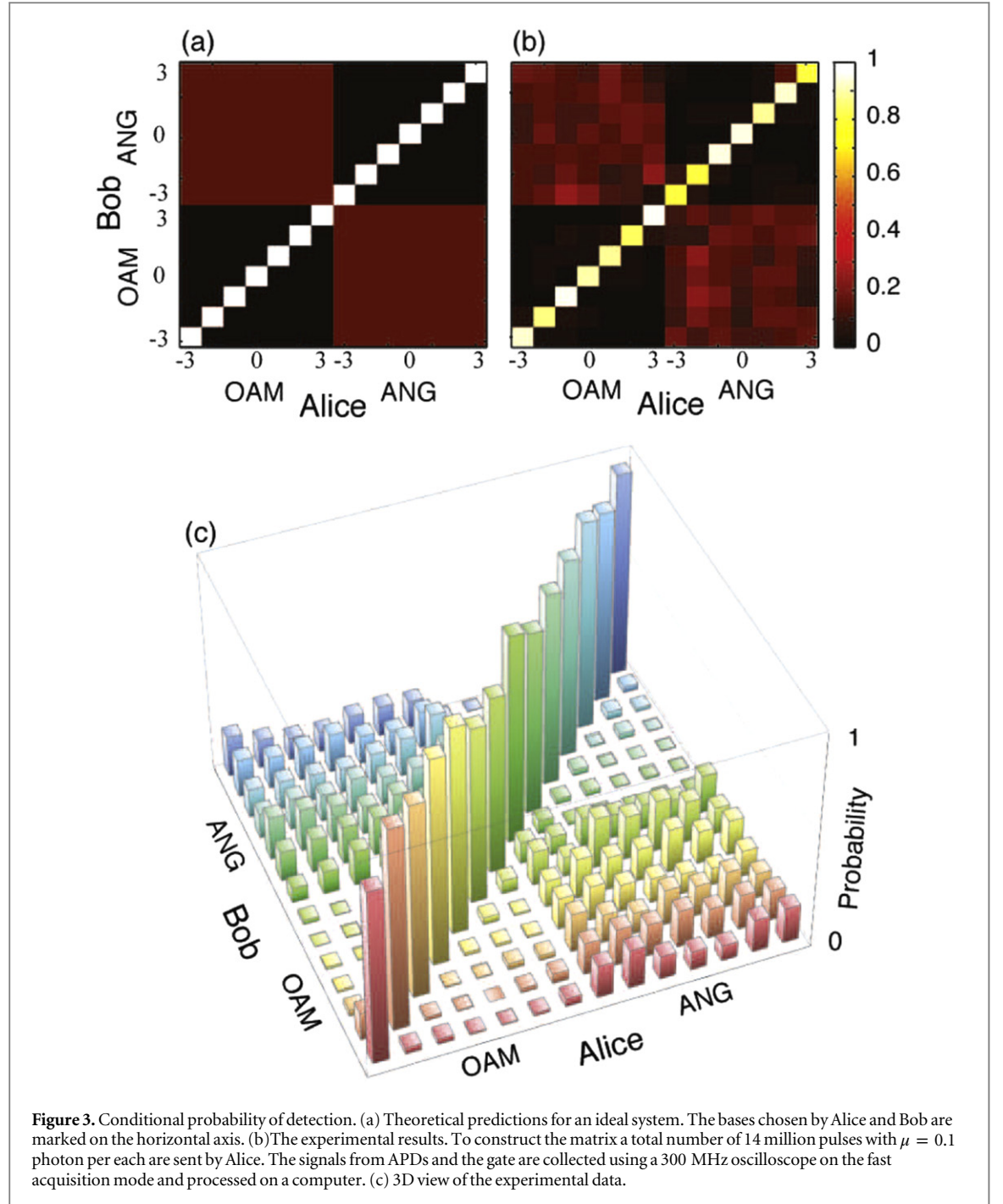
3. Security analysis

Transmission and detection efficiency

The power transmission efficiency of the mode sorter's refractive elements is measured to be 85%. Two Holoeye PLUTO phase-only SLMs are used for realizing the holograms for the fan-out element and its corresponding phase-correcting element. In addition, two cylindrical lenses are realized on the SLMs to adjust the aspect ratio of the transformed beams. The diffraction efficiency of each SLM is measured to be approximately 45%.

The fiber array consists of 7 multi-mode fibers with $62.5/125\ \mu\text{m}$ core/cladding diameters and $\text{NA} = 0.275$. We have measured the efficiency of coupling the transformed modes to the fiber array to be approximately 18%. The detection is performed with Perkin-Elmer SPCM-AQRH-14 APDs. The quantum efficiency of the APDs is $\eta = 0.65$. The transmission efficiency of the optical link can be calculated as

⁶ Old Persian cuneiform writing from the Xerxes tablet (Persia, circa 470 BC). Photo courtesy of Wendy Harns via flickr.



$$T_{\text{link}} = 0.85 \times (0.45)^2 \times 0.18 = 0.031. \quad (3)$$

Each detector has a typical dark-count rate of 50 c s^{-1} and an after-pulsing probability of 0.3%.

Classical information capacity

Figure 3 shows the conditional probability of Bob detecting each mode as a function of the mode sent by Alice. Theoretical values for the case of a system with no errors is shown on the left for comparison. In order to measure the SER more precisely, each row of the matrix is constructed by sending the same symbol many times and detecting all possible outcomes. This scheme eliminates the time consuming procedure of switching among different spatial modes and permits a much more accurate measurement of the error-rate using a large set of sent and received symbols.

The mutual information between the sent and received symbols is defined as

$$I_{AB} = \sum_{i,j} P(x_i, y_j) \log_2 \left[\frac{P(x_i, y_j)}{P(x_i)P(y_j)} \right]. \quad (4)$$

Here, x_i is the event of sending symbol i and y_j is the event of detecting symbol j . Assuming a uniform probability for sending N modes and a uniform probability of an error occurring in the detection, the equation (4) can be simplified to [13]

$$I_{AB} = \log_2(d) + F \log_2(F) + (1 - F) \log_2\left(\frac{1 - F}{d - 1}\right). \quad (5)$$

Here, $F = 1 - \delta - \epsilon$ is the probability of correctly detecting each mode. The SER caused by imperfect sorting is denoted by δ and the SER due to the dark counts is shown by ϵ . For the case of our experiment, $\delta = 0.065$ and $\epsilon = 0.04$. The total SER, $1 - F$, is directly measured from data as 10.5%. We have identified the error from the imperfect sorting, δ , by repeating the experiment in the high-light level and analyzing the results after background subtraction. The error probability ϵ can be divided to 2% from stray light, 1.9% from thermally-induced dark counts, and 0.15% from after-pulsing.

Using these numbers, we calculate I_{AB} as 2.05 bits per photon. For comparison, the ideal value of I_{AB} for $d = 7$ modes is equal to $\log_2(d) = 2.8$ bits per photon. Further, the sorting mechanism by itself would result in a value of 2.29 bits per photon in the absence of any background or dark counts. The probability of correctly detecting each mode in the absence of dark counts, also known as the separation efficiency of the mode sorter, is calculated to be slightly more than 93%.

Note that the calculation of mutual information only requires the knowledge of the cross-talk and dark count values. The loss in the optical system reduces the key generation rate of the protocol. However, a uniform loss in the transmission and detection does not change the mutual information between Alice and Bob's sifted keys since the time frames with no photon-detection event are removed in the basis reconciliation procedure.

Secure key rate

We consider a cloning-based individual attack. In this situation, the mutual information between the symbols owned by Alice and Eve can be written as [13]

$$I_{AE} = \log_2(d) + F \log_2(F_E) + (1 - F_E) \log_2\left(\frac{1 - F_E}{d - 1}\right). \quad (6)$$

Here, F_E is the fidelity of Eve's cloning machine. The value of Eve's fidelity can be optimized to gain maximum information for any given SER detected by Bob. This quantity is shown to be [13]

$$F_E = \frac{F}{d} + \frac{(d - 1)(1 - F)}{d} + \frac{2}{d} \sqrt{(d - 1)F(1 - F)}. \quad (7)$$

For our experiment, $F_E = 0.43$, resulting in $I_{AE} = 0.35$ bits. For a sufficiently long ensemble of symbols owned by Alice, Bob, and Eve the secure key R is found to be [2, 44]

$$R_{\text{net}} = R_{\text{sift}} \left[I_{AB} - \max(I_{AE}, I_{BE}) \right], \quad (8)$$

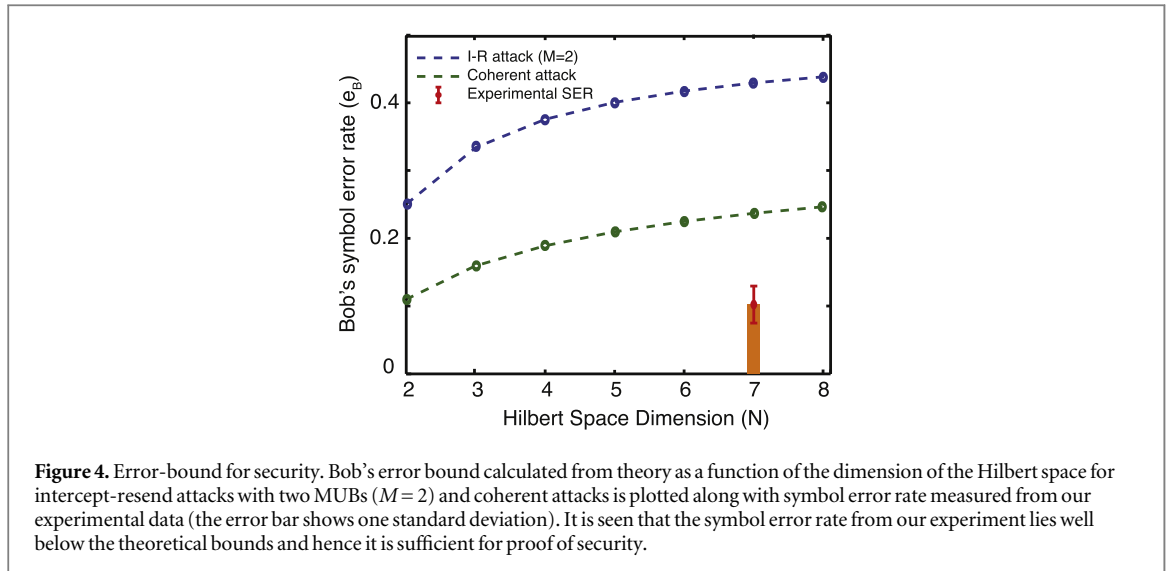
where R_{sift} is the sifted key rate. This rate can be written as a function of the pulse repetition rate f_{rep}

$$R_{\text{sift}} = \frac{1}{2} f_{\text{rep}} \mu T_{\text{link}} \eta. \quad (9)$$

For our experiment we have $\mu = 0.1$. The DMD used in our system (Texas Instrument DLP3000) is capable of switching between the computer holograms stored in its memory at the speed of 4 kHz. We refer to this mode of operation as burst mode. Burst mode can be used to transmit a short key at $f_{\text{rep}} = 4$ kHz. The internal memory can only store up to 100 patterns, which limits the applicability of the burst mode for a long key. To generate a long random key, we instead load each hologram onto the DMD using a computer. This task along with the time needed for synchronizing the two computers reduces the raw key generation rate to approximately $f_{\text{rep}} = 1$ Hz. Using $f_{\text{rep}} = 4$ kHz for the burst mode, we calculate $R_{\text{sift}} = 4$ (photons s^{-1}) and $R_{\text{net}} = 6.8$ (secure bits s^{-1}). Note that this calculation characterizes the operation of the optical system in the presence of 14 detectors for collecting data.

The calculation above can be recast to the alternative form

$$R_{\text{net}} = f_{\text{rep}} I_{\text{pulse}}. \quad (10)$$



Here, I_{pulse} is the amount of secure information transmitted per each pulse. For our experiment we infer $I_{\text{pulse}} = 1.7 \times 10^{-3}$ secure bits per pulse.

To quantitatively assess the security of our system, we plot the values for the error bound of an intercept-resend eavesdropping attack, a coherent attack, as well as the SER from our experimental data in figure 4. In an intercept-resend attack, the eavesdropper (Eve) measures the state of the intercepted photon in an arbitrarily selected basis and then resends a photon prepared to be in this same state. In a coherent attack, Eve coherently probes a finite number of qudits in order to gain information about the key [13]. It is evident from this graph that our experimental SER is well below the required bounds for security against both intercept-resend and coherent attacks (figure 4). Unlike intercept-resend attacks, the SER for coherent attacks only depends on system dimension d and is independent of the number of MUBs M [13]. Hence, increasing the number of MUBs beyond 2 results in a drop in the key rate without any gain in security against coherent attacks. Nevertheless, there is a clear increase in the allowed SER for larger system dimensions, demonstrating an advantage for using a high-dimensional encoding scheme for QKD such as that of OAM.

Using the SER, we estimate the information gained by Eve to be 0.35 bits per sifted photon for cloning-based individual attacks. It has been argued that cloning-based eavesdropping is the optimal strategy for an individual attack on systems based on qudits [13]. The portion of the key obtained by Eve is removed in the privacy amplification process, leading to a mutual information of 1.7 secure bits per sifted photon in the final key. It should be emphasized that our secure key rate analysis assumes an infinite key, while any experimental realization produces only a finite key [45]. We are working toward a finite key analysis of the security, which will be reported in the future.

In contrast to phase-only SLMs that are limited to a frame rate of 60 Hz, the DMD used in our setup has the ability to rapidly switch between modes at a speed of 4 kHz. This is especially important considering the fact that the speed of generation of spatial modes limits the key generation rate of the system. We measure our raw key generation rate to be 16.4 bits per second (for operation in burst mode). After performing basis reconciliation and privacy amplification for a sufficiently long key, we estimate the secure key rate to be 6.5 bits per second, which is more than 3 orders of magnitude larger than that achieved in previous spatial-mode based protocols [20].

Photon number splitting (PNS) attacks

The analysis above considers intercept-resend and cloning based attacks. The PNS attack is yet another possibility when the protocol uses imperfect single-photon sources. In our protocol, weak coherent pulses (WCPs) are used for realizing approximate single photon pulses. For small values of photon-number expectation values, a WCP contains either zero or one photon most of the times. However, the pulse may still contain multiple photons with a non-zero probability. In this situation, Eve can split one photon off of a multi-photon signal, without disturbing the polarization or the spatial structure of the signal [46–48]. Eve can measure her photon after basis reconciliation and obtain complete information without causing any error in the signal.

The PNS attacks pose a more serious threat in the presence of loss. In this situation, Eve can, in principle, replace the lossy channel with a perfect quantum channel and only transmit to Bob the signals of her choice. An inequality has been developed in [49] that serves as a necessary condition for security

$$p_{\text{detection}} > p_{\text{multi}}. \quad (11)$$

Here, $p_{\text{detection}}$ is the total probability of detection events for Bob, and p_{multi} is the probability of having a pulse with multi-photons. For a coherent state with an average photon number of μ , we have $P(n, \mu) = \frac{\mu^n}{n!} e^{-\mu}$, and consequently

$$p_{\text{multi}} = \sum_{n=2}^{\infty} P(n, \mu) \approx \frac{\mu^2}{2}. \quad (12)$$

The total probability of detection events can be calculated by considering the signal detection events and the detector dark counts

$$p_{\text{detection}} = p_{\text{signal}} + p_{\text{dark}} - p_{\text{signal}} p_{\text{dark}} \approx p_{\text{signal}} + p_{\text{dark}}. \quad (13)$$

Using the parameters for our experiments we have $p_{\text{multi}} = 5 \times 10^{-3}$ and

$p_{\text{detection}} = \mu T_{\text{link}} \eta + p_{\text{dark}} \simeq 2 \times 10^{-3}$. It can be seen that $p_{\text{detection}} < p_{\text{multi}}$ and hence security against PNS attacks cannot be guaranteed in our current implementation. We discuss the possible approaches for providing security against PNS attacks in the following section.

Effect of imperfect MUBs

The unbiased relation between the two bases, as defined in equation (2), guarantees that detecting a photon in the wrong basis results in a completely random outcome and hence it reveals zero information about the key. In practice, however, the imperfect generation and sorting of the OAM and ANG modes results in variations in the degree of overlap between a pair of modes chosen from the two different bases. Such variations can be noticed in the off-diagonal blocks in the matrix for conditional probability of detection (figure 3). In this situation, the measurement of a photon in the wrong basis can, in principle, reveal some information about the transmitted symbol.

The mutual information between the symbols sent in the OAM basis and detected in the ANG basis can be calculated using equation (4). For our experiment, we have calculated $I_{\text{OAM/ANG}} = 0.036$ bits per photon. Similarly, the mutual information for the case of sending a photon in the ANG basis and detecting it in the OAM basis is calculated to be $I_{\text{ANG/OAM}} = 0.058$ bits per photon. Note that these values are much smaller than I_{AB} which is equal to 2.05 bits per photon. We have assumed an unbiased relation between the OAM and ANG modes in our security analysis. The small number of the quantities $I_{\text{ANG/OAM}}$ and $I_{\text{OAM/ANG}}$ calculated above justifies the validity of this approximation. A more complete security analysis needs to take these numbers into account in estimating the information owned by Alice (I_{AE}). Such an analysis, however, is beyond the scope of current article and should be the subject of future studies.

4. Steps towards practical QKD with OAM modes

The secure key rate of a QKD system is considered as the ultimate metric for quantifying its performance. In the above sections we described how a high-dimensional encoding scheme such as that of OAM can potentially benefit the secure key rate of QKD protocols. While our experiment provides significant improvements in realizing OAM-based QKD, several challenges need to be addressed before such a protocol can be employed for practical applications. In addition to a high secure key rate, a free-space QKD link needs to provide reliable long distance operation, efficient classical post-processing, ease of alignment, and a rigorous security analysis considering the finite size of practical keys. While some of these requirements can be achieved by increasing the degree of sophistication of the system or through the use of state-of-the-art technology, there is still need for theoretical and experimental research before a full demonstration can be performed. Below, we address some of the current limitations.

Fast key generation

The secure key rate scales proportionally with the raw key generation rate. Although holography techniques can achieve kHz mode switching rates using DMDs [39], practical QKD would require key rates in the GHz regime. OAM modes can be generated and switched at MHz rates using on-chip resonators [50] and potentially at GHz rates using Q-plates [51]. However, to generate the states in the ANG basis one would need to modulate both the amplitude and phase of the beam, a task that best suits free-space holography. Recently, a method involving static holograms realized on an SLM and an AOM for switching between them achieved a MHz mode-switching rate [52]. Unfortunately, the change in the wavelength caused by the AOM forbids applying this method for QKS since side-channel attacks could be performed based on spectrum.

Alternatively, generation of OAM and ANG modes at a rate of 1 GHz or more can be achieved by illuminating a series of static holograms with beams from multiple lasers. The shaped beams after the holograms can be passively combined using a series of beam splitters. The intensity of each laser beam can then be modulated either by using electro-optic modulators or by switching diode lasers on and off [10].

High throughput

The key generation rate drops as loss increases. Moreover, high loss in the communication link makes the protocol vulnerable to PNS attacks. The throughput of our detection system can be readily increased by employing high efficiency SLMs, or AR-coated custom refractive elements. This would translate to a six-fold increase in the transmission efficiency in our experiment. Additionally, the amount of loss due to the scattering in the air can be minimized by operating in the near-infrared regime.

Turbulence mitigation

Atmospheric turbulence results in degradation of the spatial profile of the modes upon propagation. This results in mixing of the neighboring OAM and ANG modes. The effects of turbulence on OAM modes has been a topic of extensive studies [38, 53, 54]. Common solutions for mitigating the adverse effects of atmospheric turbulence include the use of every other mode for encoding [55] and utilization of adaptive optics systems [56]. Recently, long-haul free-space propagation of OAM modes has been realized using novel detection schemes [24].

Larger dimensionality

Increasing the number of the modes increases the information carried by each single photon and results in a higher secure bit rate. Previously, we have shown that our mode sorter is capable of sorting 25 OAM and ANG modes with an average mutual information of 4.17 bits per detected photons [41]. Consequently, the encoded information per photon can be readily increased by increasing the number of APDs in the experiment. Ultimately, the number of modes supported by the optical link is limited by the sizes of the transmitting and receiving apertures.

Universal security proof

A comprehensive security proof for a QKD system should include both the fundamental and practical properties of the physical system. The security analysis presented in this work assumes an infinitely long key. For a finite key, the efficiency of classical post-processing need to be measured and used for a more rigorous calculation of the secure key rate [57]. In addition, our analysis assumes a uniform error-rate and transmission efficiency for all the modes. While our data demonstrates the rationale for this approximation, a more comprehensive analysis needs to include the effects of non-uniform SER and loss in a multi-level QKD system. More research is needed to establish the theoretical framework for security analysis of such systems.

Finally, we have demonstrated security against intercept-resend and cloning-based attacks, while our implementation remains vulnerable to PNS attacks. This limitation can be avoided by either reducing the loss in the system or by employing the decoy-state protocol [58].

5. Conclusions

In conclusion, we have demonstrated that a functional QKD system based on spatial-mode encoding is realizable with current technology. We report a proof-of-principle experiment that uses a seven-dimensional alphabet encoded in OAM and in the mutual unbiased basis of ANG modes. We implement a fast mode-generation technique that uses a DMD to generate spatial modes at a speed of 4 kHz and a mode-transformation technique that is able to measure the OAM and ANG content of a photon with an accuracy of 93%. Using these two methods, we achieve a mutual information of 2.05 bits per sifted photon, which is more than twice the maximum allowable capacity of a two-dimensional QKD system. The SER of our scheme is measured to be 10.5 %, which is sufficient for proving unconditional security against coherent and individual eavesdropping attacks for an infinite key. In addition, we lay out a clear path for how our system can be enhanced to perform practical, high-dimensional QKD using current technology. For example, our SER can be significantly reduced through the use of better detectors and a more sophisticated mode-transformation technique. Our experiment opens the door to realizing real-world, multi-level quantum communication systems with record capacities and levels of security.

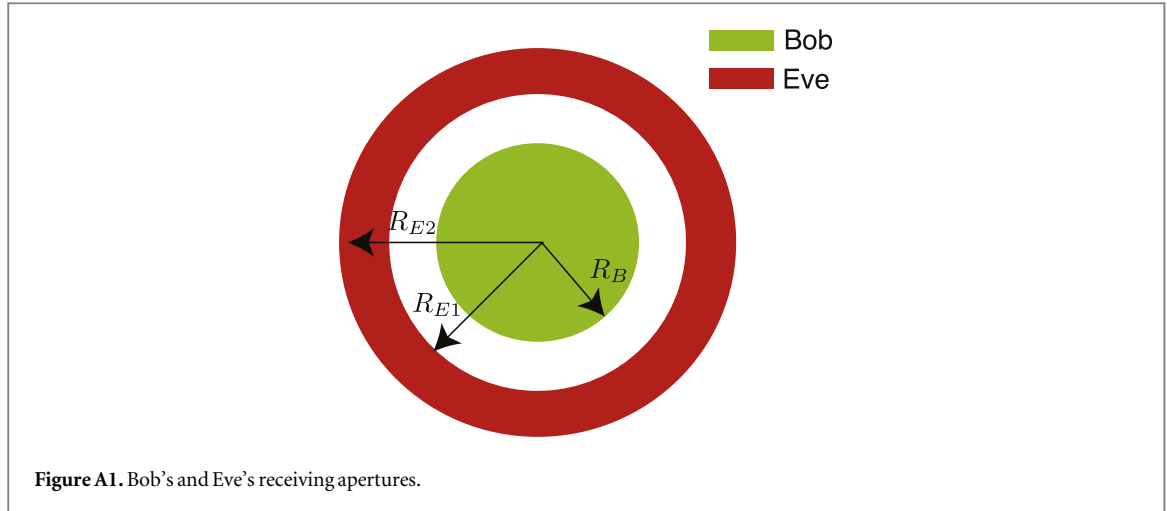


Figure A1. Bob's and Eve's receiving apertures.

Acknowledgments

We acknowledge helpful discussion with Glenn A Tyler of the Optical Sciences Company. This work was financially supported by DARPA/DSO InPho program, the US Air Force under contract FA9453-14-M-0317, the UK EPSRC under Programme Grant COAM, and the Canadian Excellence Research Chair (CERC) program. OSM acknowledges support from CONACyT. Mehul Malik acknowledges support from European Commission through a Marie Curie Fellowship.

Appendix. Diffraction and radial modes

It is known that OAM modes with larger mode index ℓ have a larger root mean squared (rms) radius in the far field [59]. Given the different radial profiles of different OAM modes, one might be concerned that the security of the protocol is compromised. More specifically, we are interested to know whether Eve can gain information by using the photons that fall outside Bob's aperture. The details of the diffraction behavior depends on the radial profile of the OAM modes as defined in the transmitter's aperture. We consider OAM modes with a top-hat intensity profile such as the ones used in our experiment. Since diffraction plays no role once the Fresnel number is sufficiently large, this issue does not directly apply to our experiment. However, the answer to the question for a low-Fresnel-number system is not trivial. Below, we show that it is impossible for Eve to gain any information by performing this attack regardless of the Fresnel number of the system.

Intercept and intercept attack

In an intercept and intercept attack (also known as denial of service) Eve detects a photon without retransmitting it. Since Alice and Bob disregards the frames with no photons in basis reconciliation, Eve will not have any mutual information with the sifted key and hence there is no loss of security.

Intercept and resend attack

In this type of attack Eve detects a photon that falls outside of Bob's apertures in a random basis. She then resends a photon in a state determined by the result of her measurement into the Bob's aperture. The geometry for Bob's and Eve's apertures are shown in figure A1. Note that the R_B , R_{E1} and R_{E2} are all bound between zero and infinity and so we are considering the most general case.

We demonstrate an OAM mode's optical field at any plane z by $\Psi_{\text{OAM}}^\ell(z)$. The probability for detecting each of the OAM modes by Eve can be written as

$$P_{\text{OAM}}^\ell(z) = \int_{R_{E1}}^{R_{E2}} |\Psi_{\text{OAM}}^\ell(z)|^2 r dr. \quad (\text{A.1})$$

Assuming Alice chooses to send OAM modes randomly with a probability of $1/d$ (where $d = 2N + 1$ is the total number of modes used), the probability for detecting any OAM mode will be

$$P_{\text{OAM}}(z) = \frac{1}{d} \sum_{\ell=-N}^N \int_{R_{E1}}^{R_{E2}} |\Psi_{\text{OAM}}^\ell(z)|^2 r dr. \quad (\text{A.2})$$

Similarly, the probability for detecting **each** of the ANG modes can be written as

$$P_{\text{ANG}}^n(z) = \int_{R_{E1}}^{R_{E2}} |\Psi_{\text{ANG}}^n(z)|^2 r dr, \quad (\text{A.3})$$

and the probability for detecting **any** ANG mode will be

$$P_{\text{ANG}}(z) = \frac{1}{d} \sum_{n=-N}^N \int_{R_{E1}}^{R_{E2}} |\Psi_{\text{ANG}}^n(z)|^2 r dr. \quad (\text{A.4})$$

We can simplify equation (A.4) using the definition of the ANG modes

$$\Psi_{\text{ANG}}^n = \frac{1}{\sqrt{d}} \sum_{\ell=-N}^N \Psi_{\text{OAM}}^{\ell} \exp\left(\frac{i2\pi n\ell}{d}\right). \quad (\text{A.5})$$

Substituting Ψ_{ANG}^n we get

$$\begin{aligned} P_{\text{ANG}}(z) &= \frac{1}{d} \sum_{n=-N}^N \int_{R_{E1}}^{R_{E2}} \left| \frac{1}{\sqrt{d}} \sum_{\ell=-N}^N \Psi_{\text{OAM}}^{\ell} \exp\left(\frac{i2\pi n\ell}{d}\right) \right|^2 r dr \\ &= \frac{1}{d} \int_{R_{E1}}^{R_{E2}} \sum_{n=-N}^N \sum_{\ell=-N}^N \sum_{\ell'=-N}^N \frac{1}{d} \Psi_{\text{OAM}}^{\ell} \Psi_{\text{OAM}}^{\ell'} \exp\left[\frac{i2\pi n(\ell - \ell')}{d}\right] r dr \\ &= \frac{1}{d} \int_{R_{E1}}^{R_{E2}} \sum_{\ell=-N}^N \sum_{\ell'=-N}^N \Psi_{\text{OAM}}^{\ell} \Psi_{\text{OAM}}^{\ell'} \sum_{n=-N}^N \frac{1}{d} \exp\left[\frac{i2\pi n(\ell - \ell')}{d}\right] r dr \\ &= \frac{1}{d} \int_{R_{E1}}^{R_{E2}} \sum_{\ell=-N}^N \sum_{\ell'=-N}^N \Psi_{\text{OAM}}^{\ell} \Psi_{\text{OAM}}^{\ell'} \delta_{\ell, \ell'} r dr \\ &= \frac{1}{d} \int_{R_{E1}}^{R_{E2}} \sum_{\ell=-N}^N |\Psi_{\text{OAM}}^{\ell}|^2 r dr \\ &= P_{\text{OAM}}(z). \end{aligned} \quad (\text{A.6})$$

The above result shows that it is equally probable for Eve to detect a photon from either the OAM basis or the ANG basis using the beam from any range of radii. Consequently, it is impossible for Eve to gain information by detecting a photon from outside of Bob's aperture. Moreover, the result remains valid at any plane z from near field to far field.

References

- [1] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. (Bangalore)* pp 175–9
- [2] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145–95
- [3] Wootters W K and Zurek W H 1982 *Nature* **299** 802–3
- [4] Dieks D 1982 *Phys. Lett. A* **92** 271–2
- [5] Takesue H, Nam S W, Zhang Q, Hadfield R H, Honjo T, Tamaki K and Yamamoto Y 2007 *Nat. Photonics* **1** 343–8
- [6] Namekata N, Takesue H, Honjo T, Tokura Y and Inoue S 2011 *Opt. Express* **19** 10632–9
- [7] Dixon A R, Yuan Z L, Dynes J F, Sharpe A W and Shields A J 2008 *Opt. Express* **16** 18790–979
- [8] Molina-Terriza G, Torres J P and Torner L 2007 *Nat. Phys.* **3** 305–10
- [9] Gibson G, Courtial J, Padgett M J, Vasnetsov M, Pas'ko V, Barnett S M and Franke-Arnold S 2004 *Opt. Express* **12** 5448–56
- [10] Wang J *et al* 2012 *Nat. Photonics* **6** 488–96
- [11] Bechmann-Pasquinucci H and Tittel W 2000 *Phys. Rev. A* **61** 062308
- [12] Bourennane M, Karlsson A and Björk G 2001 *Phys. Rev. A* **64** 012306
- [13] Cerf N, Bourennane M, Karlsson A and Gisin N 2002 *Phys. Rev. Lett.* **88** 127902
- [14] Sych D, Grishanin B and Zadkov V 2004 *Phys. Rev. A* **70** 052331
- [15] Marcikic I, de Riedmatten H, Tittel W, Zbinden H, Legré M and Gisin N 2004 *Phys. Rev. Lett.* **93** 180502
- [16] Ali-Khan I, Broadbent C and Howell J 2007 *Phys. Rev. Lett.* **98** 060503
- [17] Nunn J, Wright L J, Söller C, Zhang L, Walmsley I A and Smith B J 2013 *Opt. Express* **21** 15959–73
- [18] Zhang Z, Mower J, Englund D, Wong F N C and Shapiro J H 2014 *Phys. Rev. Lett.* **112** 120506
- [19] Walborn S, Lemelle D, Almeida M and Ribeiro P 2006 *Phys. Rev. Lett.* **96** 090501
- [20] Etcheverry S, Cañas G, Gómez E S, Nogueira W A T, Saavedra C, Xavier G B and Lima G 2013 *Sci. Rep.* **3** 2316
- [21] Shapiro J H 1974 *Appl. Opt.* **13** 2614
- [22] Miller D A B 2000 *Appl. Opt.* **39** 1681–99
- [23] Slepian D 1965 *JOSA* **55** 1110–4
- [24] Krenn M, Fickler R, Fink M, Handsteiner J, Malik M, Scheidl T, Ursin R and Zeilinger A 2014 *New J. Phys.* **16** 113028
- [25] Mair A, Vaziri A, Weihs G and Zeilinger A 2001 *Nature* **412** 313–6
- [26] Leach J, Jack B, Romero J, Jha A K, Yao A M, Franke-Arnold S, Ireland D G, Boyd R W, Barnett S M and Padgett M J 2010 *Science* **329** 662–5
- [27] McLaren M, Mhlanga T, Padgett M J, Roux F S and Forbes A 2014 *Nat. Commun.* **5** 3248

- [28] Leach J, Bolduc E, Gauthier D J and Boyd R W 2012 *Phys. Rev. A* **85** 060304(R)
- [29] Barreiro J T, Wei T C and Kwiat P G 2008 *Nat. Phys.* **4** 282–6
- [30] Malik M, Mirhosseini M, Lavery M P J, Leach J, Padgett M J and Boyd R W 2014 *Nat. Commun.* **5** 3115
- [31] Nagali E, Sansoni L, Sciarrino F, de Martini F, Marrucci L, Piccirillo B, Karimi E and Santamato E 2009 *Nat. Photonics* **3** 720–3
- [32] Mafu M, Dudley A, Goyal S, Giovannini D, McLaren M, Padgett M J, Konrad T, Petruccione F, Lütkenhaus N and Forbes A 2013 *Phys. Rev. A* **88** 032305
- [33] Groblacher S, Jennewein T, Vaziri A, Weihs G and Zeilinger A 2006 *New J. Phys.* **8** 75–75
- [34] Vaziri A, Weihs G and Zeilinger A 2002 *Phys. Rev. Lett.* **89** 240401
- [35] Vallone G, D'Ambrosio V, Sponselli A, Slussarenko S, Marrucci L, Sciarrino F and Villoresi P 2014 *Phys. Rev. Lett.* **113** 060503
- [36] Giovannini D, Romero J, Leach J, Dudley A, Forbes A and Padgett M 2013 *Phys. Rev. Lett.* **110** 143601
- [37] D'Ambrosio V, Cardano F, Karimi E, Nagali E, Santamato E, Marrucci L and Sciarrino F 2013 *Sci. Rep.* **3** 2726
- [38] Malik M, Rodenburg B, Mirhosseini M, Leach J, Lavery M P J, Padgett M J and Boyd R W 2012 *Opt. Express* **20** 13195–200
- [39] Mirhosseini M, Magaña-Loaiza O S, Chen C, Rodenburg B, Malik M and Boyd R W 2013 *Opt. Express* **21** 30196–203
- [40] Lavery M P J, Robertson D J, Berkhout G C G, Love G D, Padgett M J and Courtial J 2012 *Opt. Express* **20** 2110
- [41] Mirhosseini M, Malik M, Shi Z and Boyd R W 2013 *Nat. Commun.* **4** 2781
- [42] Brassard G and Salvail L 1994 *EUROCRYPT'93 Lecture Notes in Computer Science* vol 795 pp 410–23
- [43] Bennett C H, Brassard G, Crépeau C and Maurer U M 1995 *IEEE Trans. Inf. Theory* **41** 1915–23
- [44] Csiszar I and Korner J 1978 *IEEE Trans. Inf. Theory* **24** 339–48
- [45] Scarani V and Renner R 2008 *Phys. Rev. Lett.* **100** 200501
- [46] Yuen H P 1996 *Quantum Semiclass. Opt.* **8** 939
- [47] Huttner B, Imoto N, Gisin N and Mor T 1995 *Phys. Rev. A* **51** 1863–9
- [48] Lütkenhaus N 2000 *Phys. Rev. A* **61** 052304
- [49] Brassard G, Lütkenhaus N, Mor T and Sanders B 2000 *Phys. Rev. Lett.* **85** 1330–3
- [50] Strain M J et al 2014 *Nat. Commun.* **5** 4856
- [51] Karimi E, Piccirillo B, Nagali E, Marrucci L and Santamato E 2009 *Appl. Phys. Lett.* **94** 231124
- [52] Radwell N, Bricks D, Clark T W and Franke-Arnold S 2014 *Opt. Express* **22** 12845–52
- [53] Tyler G A and Boyd R W 2009 *Opt. Lett.* **34** 142–4
- [54] Paterson C 2005 *Phys. Rev. Lett.* **94** 153901
- [55] Rodenburg B, Lavery M P J, Malik M, Mirhosseini M, Robertson D J, Padgett M and Boyd R W 2012 *Opt. Lett.* **37** 3735–7
- [56] Rodenburg B, Mirhosseini M, Malik M, Magaña-Loaiza O S, Yanakas M, Maher L, Steinhoff N K, Tyler G A and Boyd R W 2014 *New J. Phys.* **16** 033020
- [57] Scarani V et al 2009 *Rev. Mod. Phys.* **81** 1301–50
- [58] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
- [59] Phillips R L and Andrews L C 1983 *Appl. Opt.* **22** 643